REMARKS

The above new claims are submitted to be patentable over the art of record for the following reasons. In addition, applicants thank the interview opportunity for providing a further explanation of the present invention.

Martherus's Access System does not function as an authentication authority as described in Claims 1, 6, 7, and 20

Claim 1

In the last O.A., the Examiner maintains that Martherus teaches the authentication authority means to serve as Web services powerhouse to authenticate the user identity and thus Martherus teaches the Access System as described in Claim 1.

It is the applicants' humble opinion that Martherus's system is neither designed, nor operated the same as applicants' invention. Although Martherus's system allows the user authentication across multiple domains, Martherus' system is not an authentication authority using a single authentication device as defined by applicants' invention. Instead, Martherus's system is designed to provide user access and authorization to multiple domain resources using single sign-on authentication via the use of cookie, i.e.,

Martherus (paragraph 266 lines 1-3);
"In another embodiment, "affiliate" Web Gates are installed on remote Web Servers to provide single sign-on authentication across multiple organizations.",

and Martherus (Abstract lines 1-3):
"The present invention authenticates a user for multiple resources distributed across multiple domains through the performance of a single authentication.",

and Martherus (paragraph 0012):

"One embodiment of the present invention includes receiving a request for a protected resource in a first domain. The system redirects the request to a second domain and authenticates a user for the first domain at the second domain. In one embodiment, the system transmits an authentication cookie for the second domain to the user after authentication at the second domain. In another embodiment, the system further redirects a subsequent resource request for a resource in a third domain to the second domain. The system transmits the authentication cookie to the second domain. The second domain confirms the user's authentication for the third domain using the cookie.".

Claim 6

In the last O.A., the Examiner maintains that Martherus teaches the gateway authority means and the authentication authority means comprising the use of Web services technology to be separated and placed in the Internet accessible environment to become a scalable and distributable system.

As teached by Martherus (paragraph 83 lines 7-8):
"Web Gate 28 acts as an interface between Web Server 18 and Access Server 34.",

and by Martherus (paragraph 80 lines 2-3):

> **"Web Gate 28 is a plug-in to Web Server 18. Web Gate 28 communicates with Access Server 34.",**

Martherus's Web Gate serves as a middle man or agent for the Web Server and the Access Server to communicate with each other. In applicants' system, the gateway authority acts as a network traffic load balancer to reroute authentication request messages to a different authentication authority to achieve a scalable and

distributable solution. Obviously, Martherus's Web Gate functions differently when it is compared with applicants' gateway authority. Thus, Martherus does not teach the gateway authority means as described in Claim 1.

Furthermore, although Web Server is a part of the Martherus's system, Martherus does not contain any suggestion of using the Web service technology for Web Gate to communicate with the Access Server..

Claim 7

In the last O.A., the Examiner maintains that Martherus teaches the authentication authority means contain means comprising the use of Web services technology to register and manage the user identity.

Applicants agree that Martherus teaches user registration and user identity management. However, it is under the context of achieving a single authentication solution for a centralized authentication, authorization, and auditing services, i.e.,

Martherus (paragraph 83):

"The Access Management System includes Access Server 34, Web Gate 28, Web Gate 30 (if enabled), and Access Manager 40. Access Server 34 provides authentication, authorization, and auditing (logging) services. It further provides for identity profiles to be used across multiple domains and Web Servers from a single web-based authentication (sign-on). Web Gate 28 acts as an interface between Web Server 18 and Access Server 34. Web Gate 28 intercepts requests from users for resources 22 and 24, and authorizes them via Access Server 34. Access Server 34 is able to provide centralized authentication, authorization, and auditing services for resources hosted on or available to Web Server 18 and other Web Servers."

In contrast, applicants' system is a de-centralized system. A user can register his/her identity at will with the authentication authority. The registration process

is to allow the user to synchronize an authentication client device and subsequently use the device to generate one-time identity codes. The concept of this process is foreign to Martherus.

Claim 20

In the last O.A., the Examiner maintains that Martherus teaches the authentication handler means contain means comprising the use of Web services technology to receive and process said user login request, compose and submit authority means, process and validate returned authentication response from said authentication authority means, and grant permission for said user to logon said business entities' computer.

In applicants' system, the authentication handler is designed to effectively deal with the complications aroused from the use of multiple authentication client devices to access multiple web domains and web resources. The introduction of the authentication handler with the use of a single authentication client device offers a simple and elegant means for the authentication authority to provide convenient identity authentication and verification service which is scalable and distributable. The concept of using the authentication handler with the use of a single authentication client device is completely foreign to Martherus.

Furthermore, although the function of the Web Gate as described by Martherus appears to be similar to that described in applicants' invention, the Martherus's Web Gate is designed to handle the single authentication by using the authentication cookie, i.e.,

Martherus (paragraph 0200):

"Referring back to FIG. 28, if authentication event handler 512 determines that the domain of the requested resource is a master domain (step 1032), then authentication event handler 512 attempts to authenticate at the master domain (step 1034). Otherwise, redirection event handler 504 redirects

browser 12 to the master domain (step 1036). The user then authenticates at the master domain (step 1038). The redirection and authentication of steps 1036 and 1038 are illustrated in FIG. 29 by path 1086. Upon a successful authentication at the master domain, the master domain Web Server passes an authentication cookie to the user's browser (step 1040) and re-directs the user's browser back to the first domain accessed by the user (step 1042). Also in step 1042, the master domain passes information contained in the master domain authentication cookie to the first domain in the query data portion of the redirection URL. Steps 1040 and 1042 are illustrated by paths 1088 and 1090, respectively in FIG. 29. In step 1044, the Web Gate of the first domain Web Server extracts the master domain authentication cookie information from the redirection URL, thus confirming the user's authentication at the master domain and resulting in a successful authentication (step 1046). The first domain Web Server (B.com) then sends its own authentication cookie to web browser 1082 (as depicted by path 1092) in accordance with step 780 of FIG. 22, previously described above. Any subsequent authentication by browser 1082 at domain C.com on Web Server 1074 follows the method of FIG. 28.".

Thus, there is a vast difference in the architecture design between applicants' and Martherus' system. Applicants' invention uses the single authentication client device approach, while Martherus uses the single sign-on authentication approach using cookie. Applicants' design represents a paradigm shift by emphasizing the use of a single device to achieve strong security since the single authentication approach like that used in Martherus' system can impose a great security risk if user's static password is compromised or phished.

The combination of Martherus and Guski's teaching will not produce a system that is operative for authenticating a user with one-time identity codes as described in Claim 1

As explained in the remarks of Claim 1, the Martherus's system provides a single sign-on authentication solution, while applicants' system provides a single authentication client device solution. It is obvious that the combination of Martherus and Guski's teaching can not produce a system which can provide a single client authentication device solution as described in Claim 1. Thus, applicants' invention is unobvious and patentable over the referenced prior-art.

Claim 14

The confirmation codes described in Claim 14 are used to verify the success of synchronization after the user registers his/her identities with the authentication authority. The synchronization is a process for the authentication authority to recognize the existence of the user's authentication client device. Guski's invention does not contain any information of such a process. Although the last O.A. notes that it appears that Guski's invention has a teaching of synchronization and confirmation, it is not the synchronization process described in applicants' invention, i.e.,

Guski (col. 6 lines 61-65):
"password evaluator 312 uses these quantities to regenerate the original time/date 308, which is compared with the reference time date 316",

Guski (col. 7 lines 1-3):
"the password evaluator sends a message 322 to the requesting node 102 advising of the disposition of the signon request 320".

By a close examination, it is applicants' opinion that the process described above is a process to recover/regenerate the time information and use the correct time information to generate the password. Guski did not use "synchronization" to describe this process. In contrast, the synchronization described in applicants' invention is a process used to synchronize/obtain the shared secret information without having the secret information transmitted over the wire.

As for the suggested confirmation code in Guski's teaching, it is applicants' opinion that it is merely a process to inform the **requesting node 102** about the status of the **signon request 320**. In other word, it is a process to inform the requesting node about the status of the password verification. This is not the synchronization and confirmation process as described in Claim 14.

Claim 15

The last O.A. noted that Guski appears to teach the generation of non-predictable one-time identity codes, i.e.,

Guski (col. 9 lines 22-27):

"the AP values (as well as the values of the corresponding passwords PW) for successive time values T are highly random in appearance; to a person without the key K, knowledge of the AP or password value for one time period provides no useful information about the value for another time period, even if it is the very next period.".

By a close examination, it is applicants' opinion that although Guski's system can generate random one-time passwords in appearance, Guski's one-time password is predictable in nature because these passwords are generated as a function of time which is totally predictable. The reason that Guski's one-time password is random in appearance is because of the use of the encryption technology. If a person has the knowledge of the key K, Guski's one-time password will not appear to be random.

In contrast, the generation of one-time identity codes described in Claim 15 does not involve any encryption or decryption process. Instead, applicants' invention uses a Diffie-Hellman type of algorithms, which involves the use of power and modular math operators. Furthermore, there is no one-time identity code related information in the form of encrypted or unencrypted messages being transmitted

from the authentication client device to the authentication authority in applicants' invention.

Therefore, the referenced art does not contain any suggestion that the computation of the one-time identity code could meet the requirement as described in Claim 15. This demonstrates that Claim 15 is unobvious.

The combination of Martherus, Guski and L. Brown's teaching will not produce a system that is operative for authenticating a user with one-time identity codes using a single authentication client device

As explained in the remarks of Claim 1, there are architecture differences between applicants' invention and that of Martherus's system. Applicants' invention represents a paradigm shift. The new paradigm provides a user authentication solution using a single authentication device. The old paradigm, like Martherus' system, provides a single sign-on authentication system for the purpose of sharing authorized resources over an Intranet and Extranet across multiple network domains among trusted enterprise servers. It is obvious that applicants' invention solves a different problem than that of Martherus. Thus, the combination of Martherus, Guski, and L. Brown's teaching will not produce a system that is operative for authenticating a user with one-time identity codes generated by a single authentication client device as described in Claim 1. This demonstrates applicants' invention is unobvious.

Interview Substance

On 19 April 2006, applicant (Chaing Chen) met with Examiners Mr. Patel and Mrs Truong at USPTO. Applicants greatly appreciate the interview opportunity. The purpose of the meeting is to provide a further explanation of the present invention. The agenda of the meeting is to give a) an overview of Martherus, Guski, and L. Brown's system, b) an overview of the applicant's authentication

authority system, c) a discussion of the non-obviousness nature of the applicants' system, and d) a discussion of amendments for allowance.

In the overview of Martherus' teaching, the applicant (Chaing) summarized the teaching as: a) to authenticate user for multiple resources across multiple domains, b) to perform single authentication, c) to use authentication cookie for multiple domains authentication, and d) to provide an advanced & centralized identity and access control system. The attached Fig. 1 is a schematic illustration of Martherus' system, and Fig. 2 is a diagram used to show the Martherus authentication process for multiple domains. In short, for a user to sign-on two web sites, he/she only needs to provide one password for the master domain (A.com) to authenticate his/her identity. Afterward, an authentication cookie is installed on the user's browser. This authentication cookie is the passport for the user to access the protected resources located at the second domain (B.com).

The Guski's teaching can be summarized as: a) to authenticate user using one-time identity codes, b) to use end-user device to generate one-time identity codes, c) to use invertible transformation authentication parameter to generate time dependent one-time identity codes.

The L. Brown teaching is summarized as: a) to describe the essence of the Web services (XML, SOAP, WSDL, UDDI), b) to describe an automatic invocation mechanism to integrate Web services with SQP database data access.

Subsequently, the applicant (Chaing) gave a summary of the present invention as: a) to authenticate user's identity for multiple resources across multiple web servers, b) to perform authentication using a single authenticator (authentication client device), and c) to provide a de-centralized & self-managed system to generate and verify one-time identity code. The attached Fig. 3 represents the Global Authentication Authority Architecture of the present invention. Fig. 3 is used to explain the process of how to authenticate a user's identity by Business

Web Site Server by using the global authentication authority Web services. The process is summarized as the following:

(a) registering user's public, private, and the authentication client device identities with the global authentication authority,

(b) conducting synchronization between the global authentication authority and user's authentication client device,

(c) generating an one-time identity code from the authentication client device before each logon event for authentication,

(d) submitting the one-time identity code to the business web site server,

(e) composing user identity verification request message by the authentication handler which is a plug-in software installed on the business authentication authority,

(f) submitting the identity verification request message by the authentication handler to the global authentication gateway authority using the Web services method,

(g) forwarding the identity verification request message from the global gateway authority to the global authentication authority,

(h) verifying the user's identity by the global authentication authority by checking the one-time identity code included as a part of the identity verification request message,

(i) composing identity verification response message and sending the authentication handler the response message by the global authentication authority,

(j) receiving the identity verification response message by the authentication handler,

(k) informing the business authentication authority about the verification status by the authentication handler,

(l) granting permission for the user to access protected resources by the business authentication authority upon a positive user identity verification.

As for the multiple domains authentication using the global authentication authority, Fig. 4 is the graphic representation of the process to authenticate a user by two different web sites. The process to authenticate a user is the same for all web sites. It is a repetitive procedure. Furthermore, there is no Martherus' concept of using a master domain to conduct a single sign-on authentication in applicants' invention. Apparently, the present invention provides a different approach. In fact, for a user to sign-on two web sites, he/she needs to use the authentication client device to generate two passwords and conduct two separate authentications. The salient feature of the applicants' invention is that these two passwords are generated by the same device. This simple and elegant solution can provide the user a convenient and secure means to sign-on to multiple web sites.

It is concluded that a) Martherus' system uses single authentication approach, b) applicants' system uses single authenticator (single authentication device) approach, c) the use of a single authenticator is becoming a recognized problem in today's consumer driven market, d) the combination of Martherus, Guski, and L. Brown will produce a highly centralized managed access controlled single sign-on system which is vastly different from that of the decentralized and user managed system using a single authentication device as described in applicants' invention.

In the interview meeting, Examiners pointed out the problem with the claim structure. The applicant (Chaing) thanked the feed back, suggestion and advice, and agreed to amend the claim. As a result, the new claims submitted in this response reflect the claim structure changes with a clear description that the use of the single authentication client device is a salient component for providing the authentication authority Web services. Thus, applicants have amended claims so that they are proper, definite, and define novel structure which is also unobvious. If, for any reason this application is not believed to be in full condition for allowance, applicants respectfully request the constructive assistance and suggestions such that this application can be placed in an allowable condition.